

STATEMENT OF WORK (SOW)

A. BACKGROUND INFORMATION

The US Department of Commerce, National Institute of Standards and Technology, (NIST), Intelligent Systems Division (ISD) of the Manufacturing Engineering Laboratory is working with the Information Technology Laboratory and the Electrical and Electronic Engineering Laboratory to address the information security issues of computer control systems (CCS) used in the process control industries.

This effort is being carried out through the Process Control Security Requirements Forum (PCSRF), an industry group organized under the National Information Assurance Partnership (NIAP), a joint program between the National Institute of Standards and Technology and the National Security Agency (www.niap.nist.gov). As part of the Critical Infrastructure Protection Program, NIST and NSA are working to provide technical support and assistance to industry to help improve the Nation's security posture. Creation of the PCSRf is one such effort. The PCSRf Focuses on security of the computer control systems used in process industries, including electric utilities, petroleum, pulp & paper, metals & mining, waste, water, chemicals, and pharmaceuticals, with an emphasis on industries considered to be part of the Nation's Critical Infrastructure.

Real-time computer systems used in process control applications have many characteristics that are different than traditional information processing system used in business applications. Foremost among these is design for efficiency and time-critical response. Security is generally not a strong design driver and therefore tends to be bypassed in favor of performance. A corollary is that it is generally not possible to add arbitrary additional code for security measures as a retrofit to existing systems. However, the most egregious examples of problems with process control systems are cases where nothing at all has been done, where generic passwords are left on systems, and where there are no policies or procedures for addressing security issues. Some of these issues can and should be addressed in existing systems without impacting system performance.

To address process control system information security issues, the PCSRf will seek to:

- Identify and assess threats and risks to process control information and functions
- Make security requirements recommendations for common operating environments of process control systems
- Utilize the Common Criteria for Information Technology Security Evaluation (also known as the Common Criteria, CC, or ISO 15408) for capturing the security requirements in Protection Profiles (PPs)
- Promote process control community adoption of the recommended security requirements
- Promote security awareness and integration of security considerations in the life cycle of industrial process control systems

To carry out this project, ISD requires support in helping to define the information security requirements of the process control industry and to capture the requirements as PPs utilizing the Common Criteria..

B. PURPOSE AND OBJECTIVES OF THE PROCUREMENT

The overall program objective is to reduce the vulnerability of process control systems used in key industries of the Nation's Critical Infrastructure. This procurement is to acquire services to assist NIST in defining the information security requirements of the process control industry, and to capture the requirements as PPs utilizing the Common Criteria.

C. CONTRACTOR REQUIREMENTS

The contractor will perform all tasks listed below, utilizing the Common Criteria to develop PPs to the extent practical. If conflicts arise between following the letter of the Common Criteria and making requirements understandable to industry, the Contractor shall ensure that the requirements are understandable to industry. Understandability will ultimately be determined by PCSRF participants.

Task 1: Analysis of Currently Available CCS Architectures, Including Analyses of Threats and Vulnerabilities

The Government estimates but does not guarantee that level of effort for Task 1 is 160 hours.

The contractor shall analyze computer control system architectures and equipment typically used in the process industries, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Manufacturing Execution Systems (MES); and, as part of this task, identify threats and vulnerabilities of such systems. The PCSRF will help to provide the contractor with additional information that is required.

Deliverable: 5-10 page report describing the similarities and differences between the types of systems mentioned above, with particular emphasis on the respective threats and vulnerabilities of each. In addition, the contractor shall provide a high-level assessment of the ability of these systems to protect against known threats.

Task 2: Initiate Development of Information Security Requirements

The Government estimates but does not guarantee that level of effort for Task 2 is 220 hours.

The contractor shall work with the PCSRF in the definition of systems and sub-systems of CCSs that need IT security protection. In particular, the contractor will initiate development of information security requirements for the systems/subsystems by focusing on the information included in the Identification, Overview, Target of Evaluation (TOE) description, Security Environment, and Security Objectives portion of a Protection Profile, as defined by the Common Criteria.

Deliverable: One or more partial Information Security Requirements documents, containing the elements listed above, in language and format understandable to the process control community (i.e., users and vendors).

Task 3: Completing Development of Information Security Requirements

The Government estimates but does not guarantee that level of effort for Task 3 is 220 hours.

The contractor shall work with PCSRF to define the functional and assurance requirements of such systems/sub-systems, and capture the security requirements in the Information Security Requirements documents initiated in Task 2.

Deliverable: Completed procurement language Information Security Requirements document(s) for CCS systems/subsystems that need IT security protection. Information Security Requirements document(s) shall be suitable for use as an acquisition vehicle and as a communication vehicle that is understood by the process control community (i.e., users and vendors).

Task 4: Translation of Information Security Requirements into Protection Profiles

The Government estimates but does not guarantee that level of effort for Task 4 is 150 hours.

The contractor shall translate as many as possible (at least 2) of the Information Security Requirements document(s) developed in Task 3 into Protection Profiles that can be used to enable testing and evaluation of covered CCS products/systems by accredited IT security testing laboratories.

Deliverable: Completed Information Security Requirements documents translated into Protection Profiles; as many as the contractor has time for under the existing contract.

D. GOVERNMENT RESPONSIBILITIES

Other than information provided by the PCSRF to help guide the definition of security requirements, no data, property, or equipment are anticipated to be provided by the Government for the work to be done in this procurement.

E. REPORTING REQUIREMENTS AND DELIVERABLES

Contractor will be required to provide a task deliverable for each quarter throughout the contract period:

- Quarter 1: 5-10 page report on threats and vulnerabilities of CCSs described in Section C task 1.
- Quarter 2: One or more partial Information Security Requirements documents containing the elements listed in Section C task 2.
- Quarter 3: Completed Information Security Requirements document(s) that can be used as an acquisition vehicle and as a communication vehicle (Section C task 3).
- Quarter 4: Completed Protection Profiles for CCS systems/subsystems that need IT security protection (Section C task 4).

The contractor shall provide biweekly 1-page reports of hours charged and progress made.

F. PROGRAM MANAGEMENT AND CONTROL REQUIREMENTS

- Work will be performed under the technical guidance of the Contracting Officer's Technical Representative (COTR) and in collaboration with PCSRF.
- The Contractor shall utilize the Common Criteria to the extent that understandability to the process control community is not sacrificed.

G. INSPECTION AND ACCEPTANCE CRITERIA

The COTR will review each deliverable to determine its acceptability or unacceptability, incorporating input from PCSRF participants. The submission of each deliverable will be approved or disapproved, and the contractor will be notified, within 30 days of receiving the deliverable. Deliverables that are deemed not to meet one or more requirements specified in this SOW will be rejected and the contractor will be required to correct the deficiencies at no additional cost to the government. Acceptance criteria include completeness and suitability for meeting PCSRF goals.

H. ATTACHMENTS

None.